

Reporting Module Components Overview

Authored By: Vladimir Sokol
Date: May 22, 2000
Purpose: To describe and document Reporting Module Components
Credits: Rakefet Ackerman, Sanjit Shah
Version: 1.0

Reporting Module Components Overview

The Reporting Module consists of the following components:

■ Reporting Client

(includes the Reporting Tool and the Log Consolidator Policy Editor)

■ Reporting Server

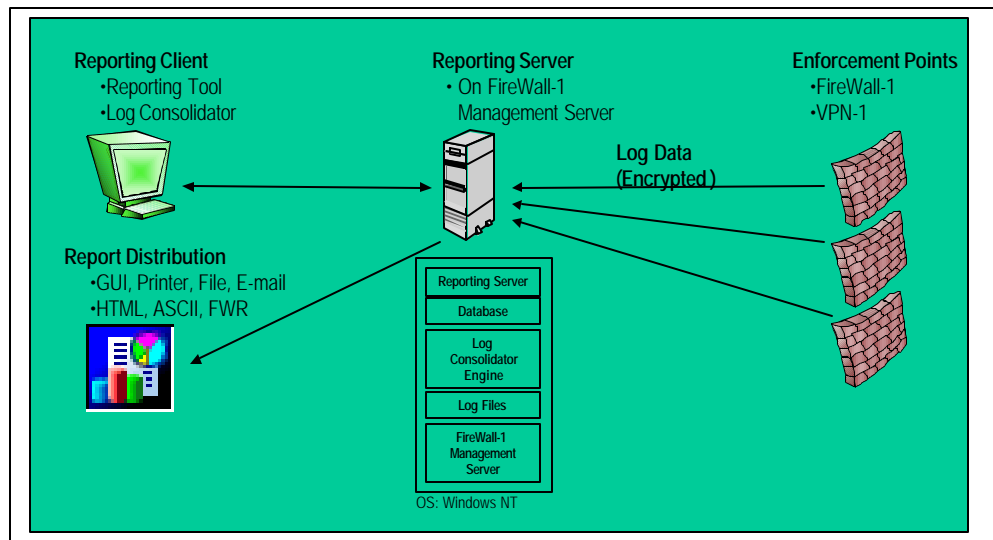
(includes the Report Server, the Database and the Log Consolidator Engine)

The Reporting Client and the Reporting Server components can be installed on the same Windows NT machine or in a Client/Server configuration to enable remote management.

In a Client/Server configuration, a Reporting Client on a Windows 95, 98 or NT machine communicates with the Reporting Server components on a Windows NT machine or a Solaris machine.

Standard Configuration

In a standard configuration, the Reporting Server components are installed on the same machine as the active FireWall-1 Management Server. A Reporting Client can be installed on separate Windows 95, 98 or Windows NT machine.



The Reporting Server components (Report Server, Log Consolidator Engine, and Database) are installed on the same machine as the active FireWall-1 Management Station. The FireWall-1 Modules send logs and alerts to the active FireWall-1 Management Server. The Log Consolidator Engine collects log data from the FireWall-1 Management Server.

System Requirements for Reporting Client

Platforms	Intel x86 and Pentium
Operating System	Windows NT (Intel only)
Disk Space	6 MB
Memory	32 MB

Reporting Server

Reporting Server is compatible with the following VPN-1/FireWall-1 Management Servers:

NT

- Check Point 2000 (VPN-1/FireWall-1 Version 4.1 SP1 and later)
- VPN-1/FireWall-1 Version 4.1
- VPN-1/FireWall-1 Version 4.0 SP2 and later

Solaris

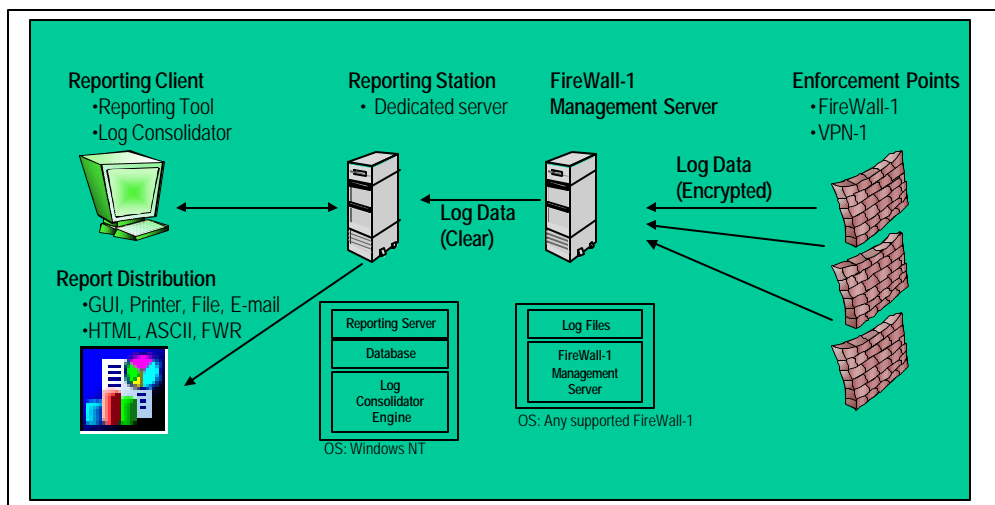
- Check Point 2000 (VPN-1/FireWall-1 Version 4.1 SP1 and later)
- VPN-1/FireWall-1 Version 4.0 SP6 and later

System Requirements for Reporting Server

	Windows	UNIX
Platforms	Intel Pentium II (233 MHz or higher)	Sun Ultra sparc 5 (360 MHz)
Operating System	Windows NT (Intel only) NTFS file system recommended	Solaris 2.5.1 (and higher)
Disk space	3 GB	3 GB
Memory	128 MB	128 MB

Standalone Configuration

Reporting Module components including Reporting Server are installed on a separate machine from the active FireWall-1 Management Server. An additional FireWall-1 Management Server dedicated to the Reporting Module system is passive — it does not manage a Security Policy for FireWall-1 Modules.



This configuration is appropriate for organizations that do not want to install the Reporting Server components on the same machine as the active FW-1 Management Server that maintains and installs the Security Policy.

All FireWall Modules send log and alert data to the active FW-1 Management Server only. The Log Consolidator Engine on the Reporting Station (which is installed on the machine with the passive FW-1 Management Server) retrieves log data from the active Management Server according to the Consolidation Policy. In this way, log messages from the FireWall Modules are not duplicated.

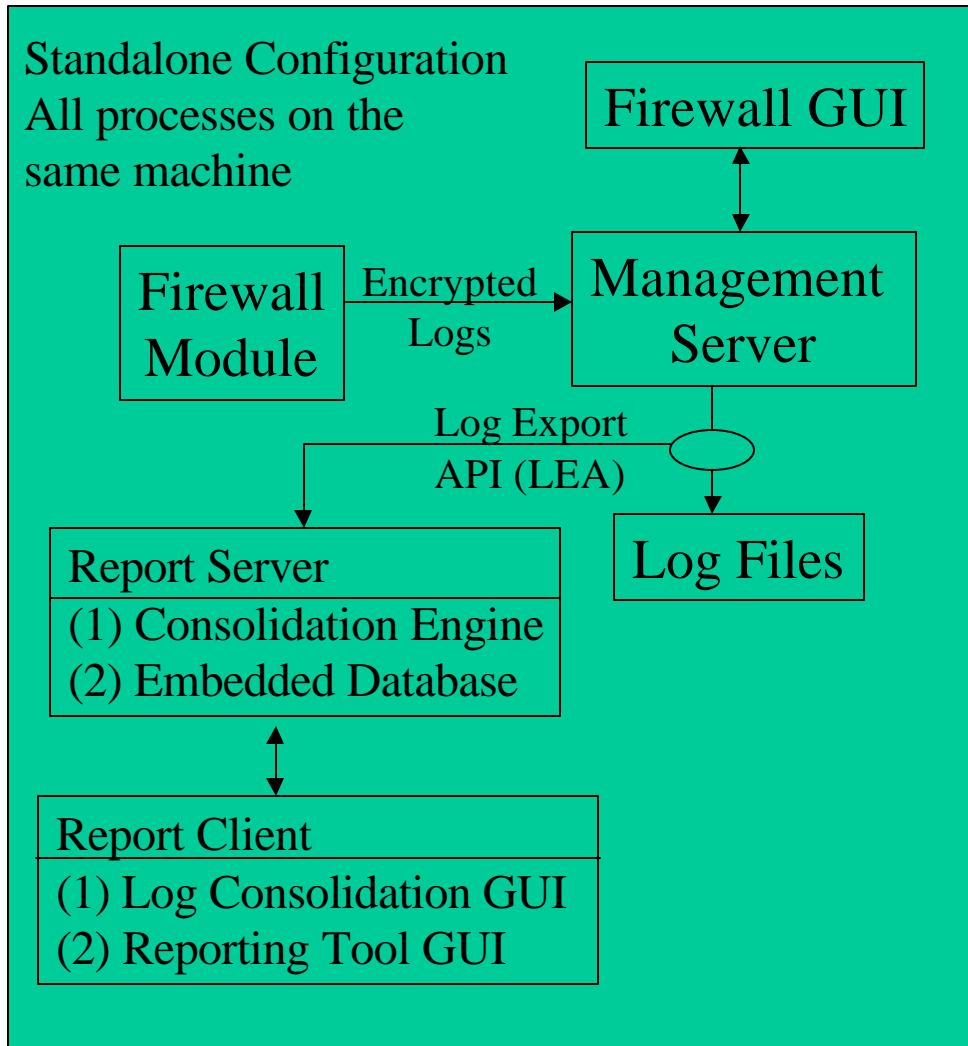
Reporting Station Components

The following components are installed on the Reporting Station:

1. Reporting Server (includes the Log Consolidator Engine, the Report Server and the Database)
2. FireWall-1 Management Server
3. Reporting Client can be installed on the Reporting Station or on a separate machine.

Note – Both the active Management Server and the secondary Management Server must be FireWall-1 Version 4.0 SP-2 or higher (Windows NT version 4.1 or higher) or FireWall-1 Version 4.0 SP-6 (Solaris) or FireWall-1 Version 4.1 SP-1 (Solaris).

Overview of System Components in a standalone Design



Alternate Configuration

Configuration with the Customer Log Module (CLM)

The Customer Log Module (CLM) was designed to allow customers or remote locations to view logs that recorded from their Internet/Intranet/Extranet Firewall.

The CLM, a scaled down Management Console, allows the customer to connect to a management console located at their facility. Logs may be sent to any of the following:

- * Management Console/Customer Managed Add-on
- * Logs are sent to the MC/CMA by default.
- * Customer Log Module
- * FW-1 V4.0 SP5 allows for a "\$FWDIR/conf/loggers" file to be created. This file will control where logs will be sent when the firewall system boots.
- * Maintained on the Firewall (Logs are stored on the local firewall for off-hour processing)

Any one or all of the above may be utilized at the same time.

Customer Log Module Architecture

The CLM exists today on any system that runs a Management Console: (AIX, HPUX, Solaris, NT). Both Customer A and Customer B firewalls report logs back to the respective CMA and the CLM.

